

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|

# MULTIMEDIA UNIVERSITY

## FINAL EXAMINATION

TRIMESTER 3, 2018/2019

**TCS2251 – COMPUTER SECURITY**  
( All Sections / Groups )

31 MAY 2019  
9.00AM - 11.00AM  
(2 Hours)

---

### INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 pages (including cover page) with 6 Questions only.
2. Attempt **ALL** questions. The distribution of the marks for each question is given. This paper carries **60 marks**.
3. Please print all your answers in the Answer Booklet provided.

**Question 1 (10 Marks)**

- a) Identify any THREE common controls of security. [3 marks]
- b) Worms and virus are the two popular malicious programs. Briefly describe the characteristics of these two. [4 marks]
- c) Your organization system is facing a serious attack due to the programming flaws, known as Incomplete Mediation. State TWO possible consequences of Incomplete Mediation. [3 marks]

[TOTAL = 3 + 4 + 3 = 10]

**Question 2 (10 Marks)**

- a) Explain THREE key drawbacks of directory implementation. [3 marks]
- b) Corporate *ABC* computer system is merely protected by password. As a security professional, you understand that this password usage should be replaced with biometrics protection. Comprehend THREE advantages of using biometrics authentication. [3 marks]
- c) You discover that your organization computer system that is protected using password is hacked. Interpret FOUR steps that an attacker usually performs to attack passwords. [4 marks]

[TOTAL = 3 + 3 + 4 = 10]

*Continued ...*

**Question 3 (10 Marks)**

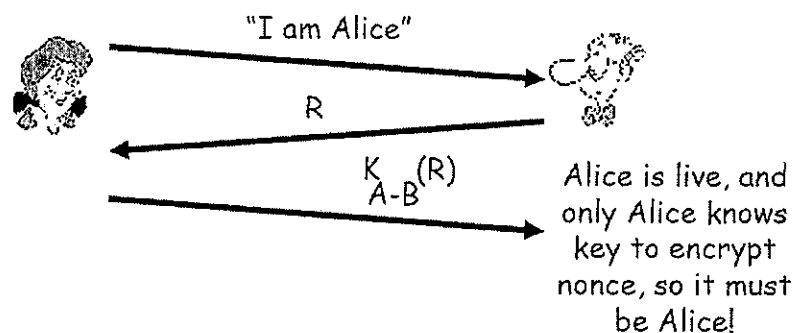
- a) The protocol below is the authentication protocol that is currently being implemented in your corporation. However, it is not secure. Explain why. Propose a more secure authentication protocol. Illustration and description on your proposed protocol may be useful.

[hint: The challenges/ limitations of the protocol may be included]

[6 marks]

Nonce: number (R) used only *once -in-a-lifetime*

4.0: to prove Alice "live", Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key



- b) Given the key "spectacular", apply monoalphabetic substitution cipher to encryption the following message: I AM AWESOME

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| s | p | e | c | t | a | u | l | r | b | d | f | g | h | i | j | k | n | n | o | q | v | w | x | y | z |

[2 marks]

- c) Given the keyword "deceptive", compute encryption to the message "we are d" by using Vigenere cipher. Vigenere Tableau is provided below. [2 marks]

*Continued ...*

Table 2.4 The Modern Vigenere Tableau

|   | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| b | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| c | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| d | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| e | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| f | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| g | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| h | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| i | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| j | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| k | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| l | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| m | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| n | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| o | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| p | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| r | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| s | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| t | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| u | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| v | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| w | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| x | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

[TOTAL = 6 + 2 + 2 = 10]

**Question 4 (10 Marks)**

- a) Your company is interested to purchase an intrusion detection system (IDS) and has asked you to propose a suitable one. They want an IDS which can detect attempts to exploit new and unforeseen vulnerabilities. Suggest the type of IDS they should purchase. Explain THREE (3) reasons why you have chosen that type of IDS and give an example of a scenario which requires this type of IDS.

[5 marks]

- b) Give TWO (2) examples of common threats on a network.

[2 marks]

- c) Suggest THREE (3) ways an attacker can impersonate a user on a network.

[3 marks]

[TOTAL = 5 + 2 + 3 = 10]

*Continued ...*

**Question 5 (10 Marks)**

- a) Briefly describe THREE(3) methods of protection to ensure the element integrity of a database. [6 marks]
- b) Suggest TWO (2) problems of controlling access using a firewall. [4 marks]

[TOTAL = 6 + 4 = 10]

**Question 6 (10 Marks)**

In the following scenarios, suggest the type of intellectual property rights the following people should apply for and give your reasons to justify why they should choose that form of intellectual property protection:

- a) Rhett is a software engineer and has developed a new mobile app to revolutionize the way we do m-commerce. [4 marks]
- b) Chiara has developed a new method to authenticate users who are disabled. [3 marks]
- c) Lara has just started a company which sells customized software solutions for organizations. [3 marks]

[TOTAL = 4 + 3 + 3 = 10]

**END OF EXAM PAPER**